DETAILED ACTION

The instant application having Application No. 10/532,193 is presented for examination by the examiner. The petition for revival filed 12/23/09 has been accepted. Consequently the amendments filed 11/19/09 have been entered. Claims 1-4 have been amended and are pending.

Response to Amendment

Claim Rejections - 35 USC § 112

The previous claim rejection under 35 USC 112 have been withdrawn due to the claim amendments filed 11/19/09.

Response to Arguments

Applicant's arguments filed 11/19/09 have been fully considered but they are not persuasive. The following interpretation of the prior art is solely based on the current set of claims and arguments submitted by the Applicant. It is not the only possible interpretation of the prior art and may be altered when/if the claims and/or arguments change.

Applicant has alleged that Menezes fails to teach an encrypted first symmetric key which is generated from the encryption of said first symmetric key with a second symmetric network key known only by at least one device of a second type connected to said network. The arguments assume that this limitation requires that the first device of the first type not know the second symmetric network key. First of all, Examiner disagrees that this limitation requires such a narrow interpretation. This limitation only requires that the second symmetric network key is known by at least one device of the second type. It says nothing as to whether the first device of a first type knows the key or not. However, even if the claim were amended to support the arguments' position, Examiner finds this interpretation of the claim to be taught as well by Menezes. In the Non-final Office Rejection filed 5/8/09, Examiner cited the pages from Menezes from 497-553. On page 503, now included for Applicant's convenience[1], Menezes teaches the Needham-Schroeder shared-key protocol. In said protocol, sender A transmits the encrypted symmetric key, k, to B. The symmetric key, k, is encrypted with a key known only to B. It is not known to the device of type A.

As such, Examiner must respectfully disagrees with Applicant's allegation and maintain that the claims do not require more than what is taught by Menezes and Patel.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

[1] See Appendix for page 503 of Menezes.

Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al. “Handbook of Applied Cryptography, PASSAGE.” Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, Fl, CRC Press, US, 1997, pages 497-553, hereinafter Menezes, in view of USP Application Publication 2005/0025091 to Patel et al., hereinafter Patel.

As per claim 1, Menezes teaches a method for encrypting data in a communication network comprising a device of a first type [A] containing:

a first symmetric key [session key, k] for encrypting the data to be sent to a device of a second type [B] connected to the network (pg. 503) wherein said second type of device is a different device type from said device of a first type; and

an encrypted first symmetric key which generated from the encryption of said first symmetric key with a second symmetric network key [E_{KBT}] known only by at least one device of a second type connected to said network [session key encrypted by key E_{KBT}(k,A); pg. 503];

the method comprising the steps that consist, for the device of a first type, in:

(a) generating a random number [Na, Nb]; pg. 503] ;

(c) encrypting the data to be transmitted with the new symmetric key [data is encrypted with k; pg. 503]; and

(d) transmitting to a device of a second type [B], via said network:

the data encrypted with the new symmetric key [session key, k, is used to encrypt the data, therefore it is inherent data will be encrypted; pgs 497-503]

the random number [Nb; pg. 503]; and

said encrypted first symmetric key [E_{KBT}] (pg. 503, protocol message 3).

Menezes is silent in disclosing computing a new symmetric key as a function of the first symmetric key and said random number. Menezes teaches the session keys needs to be updated and are a function of a random number but does not explicitly teach incorporating a previous session key into the function and a weakness of the Needham-Schroeder protocol is the freshness of k. Patel teaches one way of updating a session key is by hashing the session key with a random number to generate a new session key (0059). It is well known that session keys needs to be updated frequently to secure the system. Updating the key as taught by Patel also increases the security by not having to send the new key across the channel. Only the random number need by sent and both parties can derive the new key. This would also alleviate having to contact the trusted server for another session key. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Patel into the system of Menezes because it would provide a mechanism for securely updating the session keys.

As per claim 2, Menezes teaches the function used to compute the new symmetric key is a one-way derivation function [hk; pg. 499].

As per claim 3, Menezes teaches the function is a hash or encryption function hk; pg. 499].

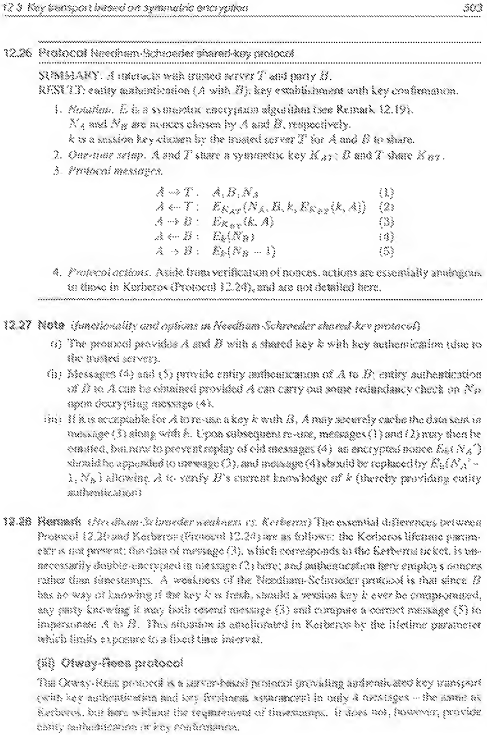
As per claim 4, Menezes teaches the device of a second type that receives data transmitted at step (d), in:

(e) decrypting, with the second symmetric network key, the encrypted first symmetric key as to produce encryption of the first symmetric key [B uses the K_{BT} to decrypt E_{KBT} to obtain k; pg. 503];

(f) determining, based on the first symmetric key obtained at step (e) and on said random number, the new symmetric key [pg. 498]; and

(g) decrypting the data received with the new symmetric key [session key is used to encrypt the data, therefore it is inherent data will be encrypted; pgs 497-499].

Appendix



12.3 Key transport based on symmetric encryption 503

12.26 Protocol Needham-Schroeder shared-key protocol

SUMMARY: A interacts with trusted server T and party B.
RESULT: entity authentication (A with B); key establishment with key confirmation.

1. *Notation.* E is a symmetric encryption algorithm (see Remark 12.19).
   N_A and N_B are nonces chosen by A and B, respectively.
   k is a session key chosen by the trusted server T for A and B to share.
2. *One-time setup.* A and T share a symmetric key K_{AT}; B and T share K_{BT}.
3. *Protocol messages.*

$$\begin{array}{lll} A \rightarrow T: & A, B, N_A & (1) \\ A \leftarrow T: & E_{K_{AT}}(N_A, B, k, E_{K_{BT}}(k, A)) & (2) \\ A \rightarrow B: & E_{K_{BT}}(k, A) & (3) \\ A \leftarrow B: & E_k(N_B) & (4) \\ A \rightarrow B: & E_k(N_B - 1) & (5) \end{array}$$

4. *Protocol actions.* Aside from verification of nonces, actions are essentially analogous to those in Kerberos (Protocol 12.24), and are not detailed here.

12.27 Note *(functionality and options in Needham-Schroeder shared-key protocol)*

(i) The protocol provides A and B with a shared key k with key authentication (due to the trusted server).

(ii) Messages (4) and (5) provide entity authentication of A to B; entity authentication of B to A can be obtained provided A can carry out some redundancy check on N_B upon decrypting message (4).

(iii) If it is acceptable for A to re-use a key k with B, A may securely cache the data sent in message (3) along with k. Upon subsequent re-use, messages (1) and (2) may then be omitted, but now to prevent replay of old messages (4), an encrypted nonce $E_k(N_A')$ should be appended to message (3), and message (4) should be replaced by $E_k(N_A' - 1, N_B)$ allowing A to verify B's current knowledge of k (thereby providing entity authentication).

12.28 Remark *(Needham-Schroeder weakness vs. Kerberos)* The essential differences between Protocol 12.26 and Kerberos (Protocol 12.24) are as follows: the Kerberos lifetime parameter is not present; the data of message (3), which corresponds to the Kerberos ticket, is unnecessarily double-encrypted in message (2) here; and authentication here employs nonces rather than timestamps. A weakness of the Needham-Schroeder protocol is that since B has no way of knowing if the key k is fresh, should a session key k ever be compromised, any party knowing it may both resend message (3) and compute a correct message (5) to impersonate A to B. This situation is ameliorated in Kerberos by the lifetime parameter which limits exposure to a fixed time interval.

(iii) Otway-Rees protocol

The Otway-Rees protocol is a server-based protocol providing authenticated key transport (with key authentication and key freshness assurances) in only 4 messages – the same as Kerberos, but here without the requirement of timestamps. It does not, however, provide entity authentication or key confirmation.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431